BANGALORE ELECTRICITY SUPPLY COMPANY LIMITED

"Selection of Service Provider for Sale of Smart Meters to prospective consumers on rate contract basis in retail outlets for arranging power supply to new connections (including temporary installations) along with Supply, Implementation, Commissioning of IT system for a period of 5 years & Maintenance of IT system for a period of 10 years in BESCOM Jurisdiction." vide Tender Enquiry No. BESCOM/2024-25/SE0193

Annexure B
COMMUNICATION SYSTEM

Table of Contents

1. ANNEXURE-B- COMMUNICATION SYSTEM SPECIFICATION

1.1. COMMUNICATION INFRASTRUCTURE
1.2. GENERAL REQUIREMENTS
1.3. NETWORK MANAGEMENT SYSTEM (NMS)
1.4. NMS REQUIREMENTS SPECIFIC TO HES
1.5. NETWORK PROTECTION & SECURITY
1.6. COMMUNICATION NETWORK ELEMENTS

1. Annexure-B- Communication System Specification

1.1. Communication Infrastructure

The communication infrastructure should cellular network or through RF. Communication network shall provide reliable medium for two-way communication between various nodes (Smart Meter, Gateway/Router/Access Point/ DCU (wherever applicable)) & HES. The engagement of network service provider would be in the scope of service provider to meet the performance level as given in the tender document.

The Smart Meters supplied should have provision to operate on various communication modes i.e., Cellular/ RF. Smart Meters to be supplied with communication NIC suitable for available frequency bands (Unlicensed Band in case of RF) in India. The Communication NIC should be designed in such a way that it would work for the project duration even if there are changes in cellular modes/cellular network configuration and shall meet SLA requirements as defined in Annexure – F. It would be the responsibility of Service Provider to supply the communication technology thoughtfully to avoid technology obsoleteness during project and subsequent extensions.

For clusters of New Connections, the Service Provider may consider providing the RF NIC & Gateway based communication technology, which shall provide reliable medium for two-way communication between gateway & HES.

Meter data shall be routed / collected by field devices like Smart Meters/ Gateway wherever applicable given the communication technology used and transported to HES through WAN backhaul connectivity.

1.2. General Requirements

The SP shall design / hire reliable, interference free & robust communication network. It shall be effective for providing communication in terrain, topology & the consumer density of the project site.

During designing, suitable consideration shall be kept for future expansion.

The entire infrastructure & associated civil works required for installation & commissioning of equipment/devices such as DCUs, repeaters, routers & access points etc. shall be in the scope of SP.

The network Solution deployed by the SP should have disaster recovery mechanism in place. The redundancy mechanism of HES and MDM and their disaster recovery plan shall also be highlighted by the SP. SP shall satisfy itself through the operational testing of network as a whole and its element for reliability before starting operations and billing.

The quality of installation of the various equipment & power supply wiring to all field equipment shall be as per standards/ regulations/prevailing practices of the utility. The reasonable supply of electricity needed for operation and maintenance of entire AMI system shall be provided by no cost for BESCOM.

A suitable NMS shall be built to monitor the performance of the communication network round the clock. The NMS shall provide viewing of all the networking elements deployed at site and enable configuration & parameterization of the networking devices and the nodes. In case of public network such as cellular, the web-based portal (for example Open Network platform) should be provided to have the network view at location of installed devices. The portal shall have connectivity & subscription management.

A suitable digital platform (cloud-based application) and mobile apps could be provided to support field installation and capture field related activities and to manage the field operation & maintenance activity during the contract period duly following the latest Cyber Security Guidelines from CEA from time to time in force. This platform shall manage project life cycle.

1.3. Network Management System (NMS)

The proposed NMS (for non-cellular only) shall facilitate following activities:

a) Security Management to protect systems and network from unauthorized access, manage user access, authorizing rights and privileges.
b) Viewing of all network elements deployed in the field and administrater configuration changes of the network devices and nodes through toolkits to automate the following tasks:

    i. Capture running configuration, capture start-up configuration, upload configuration.
    ii. Compare configuration
    iii. Real-time or scheduled capture of device configurations
    iv. Store historical device configurations captured and enable comparison of current device configuration against a previously captured configuration

c) Security patch management of all applications shall be encrypted and signed.
d) Performance Management to monitor network performance as specified.
e) Fault Management to recognize, isolate, log and identify fault on network and connected nodes, devices.

The NMS shall have a simple browser-based user interface to provide all the pertinent information about the system. The NMS shall not impact the availability and performance of AMI applications and shall load not more than 1% of network bandwidth and shall have secure communication.

The Network Management Software shall have following functionality:

a) It shall maintain performance & error statistics, and present this information via displays, periodic reports and on-demand reports.

b) Apart from real-time monitoring of critical network devices, the above information shall be collected and stored at user configurable periodicities i.e., 5 minutes to 30 minutes. The NMS shall be capable of storing the above data for a period of one (1) year at an interval of 5 minutes.

c) It shall maintain a graphical display for connectivity and status of peripheral devices. The monitored devices shall be configured to send SNMP (Simple Network Management Protocol) notifications, and the graphical element representing the device shall change to a different colour depending on the severity of the notification received.

d) It shall issue alarms when error conditions occur.

e) The period over which the statistics are gathered shall be adjustable by the user and the accumulated statistics shall be reset at the start of each period.

f) The statistics shall be available for printout and display after each period and on demand during the period.

g) In case more than one technology of AMI (example PLCC and RF between Smart Meter & DCU) deployed in the field. It shall maintain statistics on the performance and availability of node being delivered per AMI technology.

1.4. NMS Requirements Specific to HES

The Network Management System (NMS) function within the HES shall manage communication network and its associated devices and monitor the performance of network. This module shall provide real time information about the IP network and its associated NAN/WAN modules in the field device/s.

a) NMS shall be able to collect parameters viz. terminal status, device status, next hop information, RF signal strength, Hardware/software version numbers, communication logs/events etc. For cellular WAN network, it shall be able to constantly monitor the meter WAN module for its connectivity and signal strength and quality.

b) NMS function shall be able to perform ping & trace-route to an individual and a group of Nodes (NAN / WAN), Routers /Gateways / Access Point, DCU.

c) NMS function shall routinely check the logged in status of the end node / field device and its availability in the network for data exchange. In case of failure to get the 'alive' message from the end node/field device, it shall mark and notify the node as logged out. It shall be also possible to restart of a node (NAN/WAN) as well as trigger a hardware reset of the node.

d) NMS function should be able to collect and store monitoring profiles from End Points (NAN/WAN modules) and network devices for performance evaluation and troubleshooting purposes. Historical logs of monitored profiles shall be available analysis through standard reporting tool.
e) If GIS is enabled, then topology, location (lat./long) and status of all network nodes shall be visible on GIS map.

1.5. Network Protection & Security

The AMI Network shall have adequate cyber security measures not limited to the measures as described below. The network security would be extended to all the interfaces also.

Secure Access Controls: The system shall include mechanisms for defining and controlling user access to the applications environment. Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.

Authorization Controls: A least-privilege concept such that users are only allowed to use or access functions for which they have been given authorization shall be available.

Logging: Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc. Additionally, the access to such logs must be controlled in accordance with the least-privilege concept mentioned above, so that entries may not be deleted, accidentally or maliciously.

The overall cyber security policy and implementation shall account for:

a) Prevent unauthorized users from reading or writing data or files, executing programs or performing operations without appropriate privileges.
b) Document all user sign on procedure
c) Record all network traffic for detecting unauthorized activity, unusual activity and attempts to defeat system security (SP to propose and document what constitutes normal activity/traffic)
d) A user authentication scheme consisting of at least a user identification and password shall be required for the user to request a connection to any network node.
e) All users must be given Multi-Factor Authentication log-in.
f) GUI to provide role-based access based on user identity and user role. Shall have following types of users:

    i. Administrator
    ii. Operator
    iii. Field staff
    iv. Viewer/Guest

1.6. Communication Network Elements

VOID as only Cellular based communication is envisaged as the installations would be spread across BESCOM.

Sd/-
General Manager(Ele.)
DAS, SG&TIC,
BESCOM

*****